PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06K 9/00

A1

(11) International Publication Number: WO 00/55800

(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/US00/07076

(22) International Filing Date: 17 March 2000 (17.03.00)

(30) Priority Data:
60/125,052 18 March 1999 (18.03.99) US

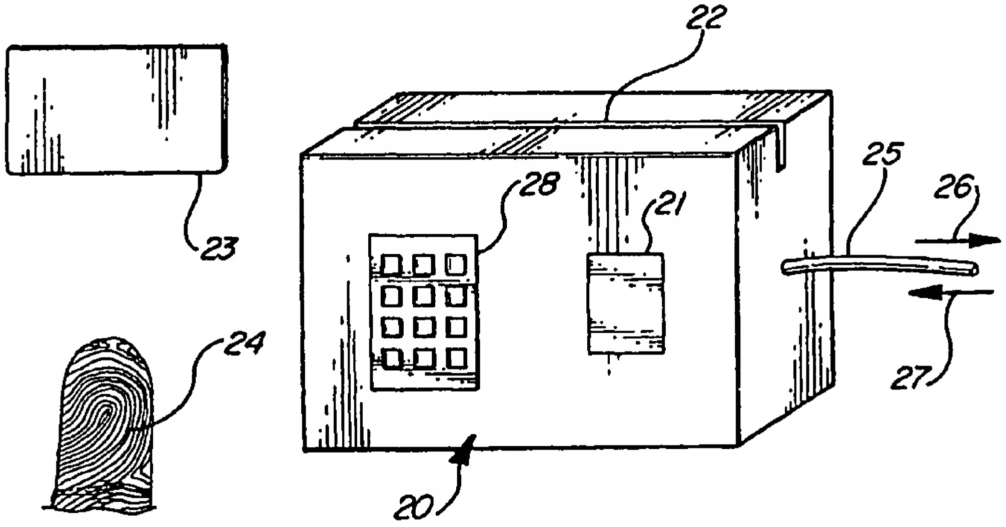
(71)(72) Applicant and Inventor: UNNIKRISHNAN, K. P. [IN/US]; 876 Oakland, Birmingham, MI 48009 (US).

(74) Agents: KRASS, Allen, M. et al.; Gifford, Krass, Groh, Sprinkle, Anderson & Citkowski, P.C., Suite 400, 280 N. Old Woodward Avenue, Birmingham, MI 48009-5394 (US).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: POINT OF SALE (POS) TERMINALS WITH BIOMETRIC VERIFICATION



(57) Abstract

A method to increase security of transactions at point of sale, i.e. POS terminals (20) by incorporating fingerprint verification. Key minutiae points from the authorized user's fingerprints (24) are extracted and stored as a template; a complete fingerprint is never stored. Minutiae extracted from the live fingerprint of a user are matched against the stored template. Upon a positive match of the two, the transaction is allowed to proceed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

POINT OF SALE (POS) TERMINALS WITH BIOMETRIC VERIFICATION

Reference to related applications

This application claims priority of U.S. provisional application serial no. 60/125,052, filed March 18, 1999, the entire contents of which are incorporated herein by reference.

Field of the invention

This invention relates generally to adding security to point-of-sale (POS) terminals and, in particular, to the use of biometrics and fingerprint recognition to achieve this security.

Background of the invention

In the current mobile and interconnected world, point-of-sale (POS) terminals are becoming widely available. POS terminals are devices such as the electronic cash registers (ECR) used in retail stores and the electronic fund transfer (EFT) terminals used in groceries and gas stations. In the ECRs, use of physical cash may be involved, while in EFTs, only "electronic cash" is involved.

Many new developments are changing the face of POS terminals and making them an integral part of our daily life. They include:

- The use of smart cards
- E-commerce, including electronic trading, online banking, and home ATMs
- New applications such as electronic benefits and loyalty programs and
- New services offering paperless transactions.

In the area of paperless transactions, documents and electronic data associated with sale, business, banking, and general retail transactions are processed and supported at remote locations, often associated with service providers. The transfer of data to and from these central locations is encrypted and there is a great need to identify/verify the user.

Currently, during transactions at POS terminals, the identity of the person is either verified through a Personal Identification Number (PIN) or the person is asked to provide a signature. With the advent of convenient fingerprint recognition technologies, and recent legislation allowing electronic verification of identities, biometric identification of the POS terminal user becomes an attractive and convenient way to ensure security of transactions. In this document we disclose fingerprint recognition methods well suited for POS terminals and describe different ways to carry out the verification process.

There have been many patents awarded for methods to increase the security of POS terminal transactions. The most relevant prior art to this invention is the U.S. patent 6,011,858 titled "Memory card having a biometric template stored thereon and system for using same" which disclosed a programmable memory card adapted to use personal information, including a fingerprint template.

U.S. patent 5,566,327 titled "Computerized theme park information management system utilizing partitioning smart cards and biometric verification" describes the use of a card of the above sort in theme parks.

U.S. patent 6,011,858 relates to memory cards and protecting the data on these memory cards using biometric templates. The primary aim of this invention is protection of data on the card. By contrast, the present invention is primarily directed to the identification of an individual through biometric means and the use of this identification to secure transactions at the POS terminal.

The fingerprint verification method of the present invention is very different from the methods disclosed in U.S. patent 6,011,858. The present method does not use the entire fingerprint to compare and does not store the entire fingerprint as templates. Instead, key characteristics of the fingerprint, called minutiae, are extracted from the fingerprint. The storage, matching, and recognition are all done using fingerprint minutiae. As soon as an image of the fingerprint is captured, information on key minutiae is extracted from it and the original fingerprint is discarded. Minutiae-based fingerprint verification has two main advantages, as described below:

1. The templates stored are very compact (about 20-30 bytes) compared to the whole fingerprint (about 65,000 bytes).
2. The verification process needs a fingerprint on the sensor, but the image of a fingerprint can never be reconstructed from its minutiae due to the feature extraction and compression, preventing the misuse of the stored information to infiltrate other fingerprint based security systems.

Summary of the invention

The present invention comprises of a method and apparatus to increase security of Point of Sale (POS) terminal transactions using a fingerprint verification (FPV) system to verify the identity of authorized users. using compact, stand-alone, fingerprint verification technologies. The central concept of this invention is the incorporation of fingerprint verification into the operation of POS terminals. We have previously disclosed very efficient methods for fingerprint recognition in U.S. patent application titled "Fingerprint verification methods and apparatus, consumer items incorporating the same", serial # 09/187,643, filed on November 6, 1998; and U.S. patent application titled "A method for fingerprint verification directly from slice data", serial # 09/262,823, filed on March 5, 1999, the entire contents of which are incorporated herein by reference. The present invention utilizes methods of fingerprint verification for enhancing the security of transactions at POS terminals.

The recognition systems described in the two pending U.S. patent applications noted above do not directly compare two fingerprints for verification. Certain key characteristics, called minutiae, are first extracted from fingerprints. These minutiae are compared against previously stored fingerprint minutiae of authorized users. The use of fingerprint minutiae also has the advantage that the individual templates are very small in size (about 50-60 bytes). A typical fingerprint is 65 K Bytes (256x256 image at 8 bits per pixel), and so by extracting key minutiae from the fingerprints, the amount of data is reduces by a factor of about 1000. Another key factor is that the fingerprint can't be reconstructed from the stored minutiae.

Again, it is the ability to incorporate compact minutia detection into the fingerprint recognition system that makes our system different from prior art. It also makes fingerprint identification safe and fraud-proof.

Although the aforementioned pending patents are the preferred method for fingerprint recognition, this invention can easily incorporate any matching technique that is suitably ported onto low-cost hardware and implemented by anyone of ordinary skill in the field. See the papers Jain, A.K., Hong, L., Pankant, S, and Bolle, R., "An Identity Authentication System Using Fingerprints", Proceedings of IEEE, vol. 85, pp. 1365-1389, 1997; Roddy, A.R., and Stosz, J.D., "Fingerprint Features – Statistical Analysis and System Performance Estimates", Proceedings of IEEE, vol. 85, pp. 1390-1422, 1997; and Blue, J.L., Candela, G.T., Grother, P.J., Chellappa, R., Wilson, C.L., and Blue, J.D., "Evaluation of Pattern Classifiers for Fingerprint and OCR Applications", Pattern Recognition, vol. 27, pp. 485-501, 1994, for some of the commonly used methods for fingerprint recognition.

Brief description of the drawings

Figure 1 is a schematic diagram of a POS terminal with a fingerprint scanner embedded in the POS terminal;

Figure 2 is a schematic diagram of a POS terminal with a card reader, a key pad, and a fingerprint scanner embedded in the POS terminal;

Figure 3 is a schematic diagram of a POS terminal with a card reader, a key pad, a fingerprint scanner, and fingerprint verification circuitry in the POS terminal;

Figure 4a is a schematic diagram of a POS terminal with a magnetic-stripe card reader, a fingerprint scanner, and fingerprint verification circuitry in the POS terminal;

Figure 4b is a schematic diagram of a POS terminal with a smart card reader, a fingerprint scanner, and fingerprint verification circuitry in the POS terminal; and

Figure 5 is a schematic diagram of a POS terminal with a smart card reader with the fingerprint scanner on the smart card, and fingerprint verification circuitry in the POS terminal.

Detailed description of the invention

Our two pending U.S. patent applications (serial # 09/187,643, and serial # 09/262,823) describe extremely compact, minutia-based fingerprint verification schemes, using non-obvious techniques.

The technique described in U.S. patent application # 09/187,643 is well suited for sensors of the size of the fingerprint. The disclosures in it include an efficient method to extract local orientation information from fingerprint images, a method to characterize a fingerprint using this information and a method to detect minutiae from it. An efficient method to recognize fingerprints from this data was also presented. It further presented hardware implementations of the above, and consumer items incorporating fingerprint recognition, not limited to one by the above method, in their design. As a result of methods disclosed in the above patent application, compact and inexpensive fingerprint recognition systems became possible.

The techniques disclosed in U.S. patent application # 09/262,823 are well suited for sensors smaller than the size of fingerprints. In that application we disclosed a method for verifying fingerprints directly from slice data. The method uses a feature detecting front-end to extract minutia information from the individual slice images of fingerprints, a bank of time-delays to organize the output of these feature detectors over time, and a set of individual recognition units to recognize each different fingerprint. The characteristics of each fingerprint in the database is stored in the pattern of connections between the time-delays and recognition units. In the above patent application we also disclosed an implementation of this method of fingerprint recognition using commercially available, inexpensive hardware. The method described in the patent disclosure allows fingerprint sensors to capture the fingerprint as thin slices and allows associated recognition systems to do the recognition directly from these slices, as and when they are captured. As a result, (i) the fingerprint sensors can be small and hence inexpensive, and (ii) the recognition systems do not need cumbersome reconstruction algorithms and hence can be implemented in inexpensive hardware. The technology described in the application made compact, low-cost, stand-alone, fingerprint verification feasible.

It is the extreme synergy between the currently available, compact, fingerprint sensors (details of which are provided later) and the extremely compact recognition systems disclosed in the pending U.S. patent applications # 09/187,643, and # 09/262,823 that makes our invention unique.

The following description of the present invention is divided into 2 sections, namely:

1. Design of a compact fingerprint recognition method, and
2. Three distinct methods (named Methods A, B, and C) to incorporate compact fingerprint recognition devices into POS terminals.

COMPACT FINGERPRINT RECOGNITION METHOD

Below is a description of each function in the process of fingerprint verification. The sensor captures an image of the fingerprint, and the recognition performs minutia detection, template storage, matching and response generation.

Sensing

The are many currently available compact, solid-state fingerprint sensors. These are the size of a full postage stamp (for example, the sensor from Authentec, Inc., described at www.autentec.com/products.htm, the sensor from Siemens, described at www.siemens.com, the sensor from ST Microelectronis, described at www.st.com/stonline/index.htm, the sensor from Veridicom, described at www.veridicom.com/ products.htm), or a slice of it (the sensor from Thomson-CSF, described at www.tcs.thomson-csf.com/US/fingerchip). An appropriate solid-state sensor provides the image of the fingerprint at a resolution of one bit (black/white) or 8 bits (256 gray levels) per pixel.

Recognition of whole fingerprints

Fingerprints consist of ridges and valleys of approximately constant width. Fingerprint minutiae are end points and bifurcation points of these ridges. Methods for extracting information about these minutiae from fingerprint images, storing them as templates of authorized users and matching minutiae from unknown fingerprints against these stored templates to verify the identity of the person are described in the U.S. patent application titled

"Fingerprint Verification Methods and Apparatus, Consumer Items Incorporating the Same", serial # 09/187,643, filed on November 6, 1998,the entire contents of which are hereby incorporated by reference.

Minutia detection

Fingerprints consist of ridges and valleys of approximately constant width. Fingerprint minutiae are end points and bifurcation points of these ridges. The methods described in the above U.S. patent application extracts information about their locations and orientations from the fingerprint image. The location information consists of their x and y co-ordinates, and the orientation information consists of the orientation of one (at end points) or three (at bifurcation points) lines at the minutiae. In the registration mode, authorized users' minutiae are stored as templates. In the verification mode, these minutiae are matched against stores templates.

Template storage

The authorized fingerprints are stored as minutia templates. In the preferred embodiment, described in the above U.S. patent application, three templates (from three different scans of the same finger) are stored for each person.

Template matching

For a new image, extract minutiae as described above in "minutia detection" along with calculating their cross-correlation (with a certain amount of translation and rotation invariance) with all stored templates. Sort the cross-correlation scores and apply the following logic:

- Are any of these cross-correlation values above a pre-determined threshold?
- If any of them do, does the next one or two belong to the same person?

If the answers are YES to both, the new fingerprint is positively verified. The complete verification system, as described above, runs in real-time on an inexpensive 16 or 8 bit micro controller.

Any other suitable matching technique can also be used (see the paper Jain, A.K., Hong, L., Pankant, S, and Bolle, R., "An Identity Authentication System Using Fingerprints", Proceedings of IEEE, vol. 85, pp. 1365-1389, 1997 for a description of some of the matching techniques).

Recognition of fingerprint as slices

Unlike the other sensors, the sensor from Thomson-CSF, described at www.tcs.thomson-csf.com/US/fingerchip, captures the fingerprint as slices. This sensor is smaller than the size of a fingerprint. The patent application titled "A Method For Fingerprint Verification Directly From Slice Data," serial # 09/262,823, filed on March 5, 1999 discloses a method to recognize the fingerprints directly from the slices, without any elaborate reconstruction. This method uses time-delays to combine the minutia information from individual slices. This method can be used when the sensors are smaller than the fingerprint and when the finger has to be slid past the sensor.

POINT OF SALE (POS) TERMINALS INCORPORATING COMPACT FINGERPRINT RECOGNITION METHODS

We now describe three methods, identified as method A, method B, and method C, to incorporate fingerprint recognition into POS terminals. In method A, fingerprint-template storage and matching with minutiae extracted from a fingerprint captured at a POS terminal are done centrally, while in methods B and C, the matching is done locally, at the POS terminal. The difference between methods B and C is that in method B, the templates are stored centrally and brought over to the POS terminal, while in method C, no templates are stored at a central location. In all three methods, the minutia information is extracted from the fingerprint at the POS terminal.

Method A: Minutia storage and matching done centrally

FIG. 1 schematically shows a POS terminal 10 incorporating method A. The POS terminal 10 has a fingerprint sensor 11 incorporated into it. The customer places his/her finger 12 on the sensor 11. The POS terminal 10 captures an image of the fingerprint. The POS terminal 10 contains all necessary circuitry to extract key minutiae information and transmits this information 14 (over telephone wires 13 or via another suitable medium) in a suitably encrypted form to a central computer at a remote location. The central computer identifies the fingerprint and transmits the identity and other relevant information to the POS terminal 10. The POS terminal 10 completes the transaction after receiving a positive verification 15 from the central computer.

FIG. 2 shows a modification of the above method, where, in addition to providing a fingerprint 24, the person may also enter an identifying code at the

POS terminal 20. This additional information is entered either using a keypad 28, where the customer for example enters a PIN or account number, or by swiping a card 23 containing this information stored on it. The POS terminal 20 contains all necessary circuitry to extract key fingerprint minutiae information and transmits this information and the PIN 26 (over telephone wires 25 or via another suitable medium) in a suitably encrypted form to a central computer at a remote location. The central computer performs an authentication (i.e. verifies he/she is the person identified by the PIN 26). The POS terminal 20 completes the transaction after receiving a positive authentication 27 from the central computer. Since authentication involves only matching one template against the incoming fingerprint minutiae, the total amount of computation at the central computer is cut down drastically.

Method B: Central minutia storage and local matching

FIG. 3 schematically shows the configuration of a POS terminal 30 where the fingerprint verification is performed at the terminal itself. Only the result of this verification is transmitted to the central computer. The user first enters identifying information about himself by entering a PIN or account number using the keypad 38 or by swiping the card 37 containing this PIN/account number. This information 34 is immediately sent over to the central computer, and the central computer sends back the minutia information 35 associated with that account or PIN. The user puts his finger 32 on the fingerprint sensor 31 in the POS terminal 30. This fingerprint is compared against the template 35 brought over from the central computer, and the verification result 36 is transmitted back to the central computer. The advantage of such a system is that all templates are stored centrally and available at all terminals. The PIN/account number 34 is very small in size (few bits) and can be transmitted to the central computer very quickly. The minutia template associated with each PIN/account number is also very small (50-100 Bytes) and can be brought over to the POS terminal 30 very quickly. All these can be done while the fingerprint 31 is captured and processed at the POS terminal 30. The verification can be done immediately and the whole transaction proceeds with no substantial wait.

Method C: Entire matching done locally at the POS terminal

This method is shown schematically in FIG. 4a, and FIG. 4b. In FIG. 4a, the magnetic stripe card 41 carries, in addition to the account/PIN information, the minutia template of the person's fingerprint. He swipes the card 41 through the slot 42 and the POS terminal 40 gets the account and minutia information from the card 41. The user subsequently puts his finger 45 on the sensor 46 in the POS terminal 40. The terminal performs the minutia-matching and optionally sends out a result 48 to a central computer via the telephone link 47 or another suitable medium. The central computer optionally sends any information 49 needed (e.g., authorization) back to the POS terminal 40.

In FIG. 4b, the smart card 43 carries, in addition to the account/PIN information, the minutia information of the person's fingerprint. He puts the card 43 in the slot 44 and the POS terminal 40 gets the account and minutia information from the card 43. The user subsequently puts his finger 45 on the sensor 46 in the POS terminal 40. The terminal performs the minutia-matching and optionally sends out a result 48 to a central computer via the telephone link 47 or another suitable medium. The central computer optionally sends any information 49 needed (e.g., authorization) back to the POS terminal 40.

The main advantage of the above configurations is that the entire fingerprint verification is done at the POS terminal 40, independent of the central computer. There is no data or very minimal (few bits) amount of data (48 and 49) to be transmitted between the terminal 40 and the central computer. There is no central storage of fingerprints, and hence no "big brother" fears. When the card is initially issued to the person at a facility, his fingerprint is scanned, key minutia information extracted from it, and these minutiae are securely stored on the card.

Another configuration is shown in FIG. 5. The fingerprint sensor 52 is on the card 51, instead of on the POS terminal 50. The user places the card 51 in the card-reader 55, with is finger 53 on the fingerprint sensor 52. The POS terminal 50 first gets the account information and then the minutia information from the card 51. The fingerprint image is captured and compared at the POS terminal 50. The result of verification 57 is optionally transmitted to the central computer via a telephone link 56 or another suitable medium. Optionally, the central computer sends an authorization information 58 back to the terminal 50. The POS terminal 50 may record information the transaction on the card 51. The advantage of this method is that the same sensor 52 (the one on the user's card 51) is used to create the minutia template of the authorized user and subsequently in every verification. As a result, errors due to differences in sensors are eliminated. For example, different sensors may have different noise characteristics and different image quality. The smart card used in this configuration may be of the existing "multi-app" kind which draws the necessary power from the terminal as the user places it in the card reader, or a future kind with its own battery power.

While this invention has been described and illustrated herein with respect to preferred embodiments, it is understood that alternative embodiments and substantial equivalents are included within the scope of the invention as defined by the appended claims.

I claim:

1. A biometrically enabled point-of-sale (POS) terminal comprising:

imaging circuitry to image a fingerprint of a person seeking authorization to initiate a transaction;

circuitry to extract minutiae information from an image of the fingerprint produced by the fingerprint sensor;

communication circuitry between the POS terminal and a central computer which contains a database of fingerprint templates for all authorized persons; and

comparison circuitry in the central computer to compare minutiae information sent by the POS terminal to the fingerprint templates stored in the database of the central computer and to generate a signal based on results of the comparison.

2. The biometrically enabled point-of-sale (POS) terminal as in claim 1, wherein the imaging circuitry comprises a fingerprint sensor.

3. The biometrically enabled point-of-sale (POS) terminal as in claim 1, further comprising encryption circuitry to encrypt the minutiae information prior to sending it to the central computer.

4. The biometrically enabled point-of-sale (POS) terminal as in claim 1, further comprising decryption circuitry to decrypt the minutiae information sent by the POS terminal to the central computer.

5. The biometrically enabled point-of-sale (POS) terminal as in claim 1, wherein the image of the fingerprint generated by the fingerprint sensor is in the form of a bitmap.

6. The biometrically enabled point-of-sale (POS) terminal as in claim 1, wherein the templates stored in the central computer are the minutiae information corresponding to each fingerprint.

7. The biometrically enabled point-of-sale (POS) terminal as in claim 1, wherein the minutiae information extracted from each fingerprint are compared with the minutiae information in each fingerprint template stored in the central computer to authorize a person to proceed with a transaction.

8. A biometrically enabled point-of-sale (POS) terminal comprising:

keyboard circuitry to enter an identification number corresponding to the person seeking authorization into the POS terminal;

communication circuitry to send the identification number to the central computer in order to identify the stored fingerprint template corresponding to the identification number;

circuitry to select the stored fingerprint template corresponding to the identification number;

imaging circuitry to image a fingerprint of a person seeking authorization to initiate a transaction;

circuitry to extract minutiae information from an image of the fingerprint produced by the fingerprint sensor;

communication circuitry to send extracted minutiae information to a central computer which contains a database of fingerprint templates for all authorized persons; and

comparison circuitry in the central computer to compare the extracted minutiae information with the selected fingerprint template.

9. The biometrically enabled point-of-sale (POS) terminal as in claim 8, further comprising circuitry to generate a signal based on results of the comparison between the extracted minutiae information and the stored fingerprint templates.

10. The biometrically enabled point-of-sale (POS) terminal as in claim 8, further comprising encryption circuitry to encrypt the minutiae information prior to sending it to the central computer.

11. The biometrically enabled point-of-sale (POS) terminal as in claim 8, further comprising decryption circuitry to decrypt the minutiae information sent by the POS terminal to the central computer.

12. A biometrically enabled point-of-sale (POS) terminal comprising:

imaging circuitry to image a fingerprint of a person seeking authorization to initiate a transaction;

circuitry to extract minutiae information from an image of the fingerprint produced by the imaging circuitry;

keyboard circuitry to enter an identification number into the POS terminal corresponding to the person seeking authorization;

communication circuitry to send the identification number to the central computer in order to identify the stored fingerprint template corresponding to the identification number;

circuitry to select the stored fingerprint template corresponding to the identification number and to send the stored template to the POS terminal; and

circuitry to compare the extracted minutiae information to the selected fingerprint template in the POS terminal.

13. The biometrically enabled point-of-sale (POS) terminal as in claim 12, further comprising circuitry to generate a signal based on results of the comparison between the extracted minutiae information and the stored fingerprint templates.

14. The biometrically enabled point-of-sale (POS) terminal as in claim 12, further comprising encryption circuitry to encrypt the stored fingerprint template prior to sending it to the POS terminal.

15. The biometrically enabled point-of-sale (POS) terminal as in claim 12, further comprising decryption circuitry to decrypt the stored fingerprint template sent by the central computer in the POS terminal.

16. A biometrically enabled point-of-sale (POS) terminal comprising:

identification card to store a fingerprint template on the card for a person seeking authorization to initiate a transaction prior to the initiation of the transaction;

a card reader configured to transfer the stored fingerprint template from the card to the POS terminal;

imaging circuitry on the POS terminal to image a fingerprint of the person seeking authorization;

circuitry to extract minutiae information from the image of the fingerprint captured by the fingerprint sensor in the POS terminal; and

circuitry to compare the extracted minutiae information to the stored fingerprint template using POS terminal circuitry.

17. The biometrically enabled point-of-sale (POS) terminal as in claim 16, wherein the image of the fingerprint generated by the fingerprint sensor in the POS terminal is in the form of a bitmap.

18. The biometrically enabled point-of-sale (POS) terminal as in claim 16, wherein the fingerprint template stored in the identification card is in

the form of minutiae information corresponding to the person seeking authorization.

19. A biometrically enabled point-of-sale (POS) terminal comprising:

smart card circuitry to store a fingerprint template on a smart card for a person seeking authorization to initiate a transaction prior to the initiation of the transaction;

an opening in the POS terminal for inserting the smart card into the POS terminal;

circuitry to transfer the stored fingerprint template from the smart card to the POS terminal;

imaging circuitry on the POS terminal to image a fingerprint of the person seeking authorization;

circuitry to extract minutiae information from the image of the fingerprint captured by the fingerprint sensor in the POS terminal; and

circuitry to compare the extracted minutiae information to the stored fingerprint template using POS terminal circuitry.

20. The biometrically enabled point-of-sale (POS) terminal as in claim 19, wherein the image of the fingerprint generated by the fingerprint sensor in the POS terminal is in the form of a bitmap.

21. The biometrically enabled point-of-sale (POS) terminal as in claim 19, wherein the fingerprint template stored in the smart card is in the form of minutiae information corresponding to the person seeking authorization.

22. A biometrically enabled point-of-sale (POS) terminal comprising:

smart card circuitry to store a fingerprint template on a smart card for a person seeking authorization to initiate a transaction prior to the initiation of the transaction;

an opening in the POS terminal for inserting the smart card into the POS terminal;

circuitry to transfer the stored fingerprint template from the smart card to the POS terminal;

imaging circuitry on the smart card to image a fingerprint of the person seeking authorization;

circuitry to extract minutiae information from the image of the fingerprint captured by the fingerprint sensor on the smart card; and

circuitry to compare the extracted minutiae information to the stored fingerprint template using POS terminal circuitry.

23. The biometrically enabled point-of-sale (POS) terminal as in claim 22, wherein the image of the fingerprint generated by the fingerprint sensor in the smart card is in the form of a bitmap.

24. The biometrically enabled point-of-sale (POS) terminal as in claim 22, wherein the fingerprint template stored in the smart card is in the form of minutiae information corresponding to the person seeking authorization.

25. A method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal comprising:

imaging a fingerprint of a person seeking authorization to initiate a transaction using a fingerprint sensor;

extracting minutiae information from an image of the fingerprint produced by the fingerprint sensor;

communicating extracted minutiae information to a central computer which contains a database of fingerprint templates for all authorized persons; and

comparing minutiae information sent by the POS terminal to the fingerprint templates stored in the database of the central computer; and

generating a signal based on results of the comparison.

26. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 25, wherein the imaging circuitry comprises a fingerprint sensor.

27. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 25, further comprising the step of encrypting minutiae information prior to sending it to the central computer.

28. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 25, further comprising the step of decrypting the minutiae information sent by the POS terminal to the central computer.

29. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 25, wherein the image of the fingerprint generated by the fingerprint sensor is in the form of a bitmap.

30. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 25, wherein the templates stored in the central computer are the minutiae information corresponding to each fingerprint.

31. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 25, further comprising the step of comparing the minutiae information extracted from each fingerprint with the minutiae information in each fingerprint template stored in the central computer and authorizing the person to proceed with a transaction based on results of the comparison.

32. A method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal comprising:

entering an identification number corresponding to the person seeking authorization into the POS terminal;

sending the identification number to the central computer in order to identify the stored fingerprint template corresponding to the identification number;

selecting the stored fingerprint template corresponding to the identification number;

imaging a fingerprint of a person seeking authorization to initiate a transaction using a fingerprint sensor;

extracting minutiae information from an image of the fingerprint produced by the fingerprint sensor;

sending extracted minutiae information to a central computer which contains a database of fingerprint templates for all authorized persons; and

comparing the extracted minutiae information to the stored fingerprint template in the central computer.

33. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 32, further comprising the step of generating a signal based on results of the comparison between the extracted minutiae information and the stored fingerprint templates.

34. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 32, further comprising the step of encrypting minutiae information prior to sending it to the central computer.

35. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 32, further comprising the step of decrypting the minutiae information sent by the POS terminal to the central computer.

36. A method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal comprising:

imaging a fingerprint of a person seeking authorization to initiate a transaction using a fingerprint sensor;

extracting minutiae information from an image of the fingerprint produced by the fingerprint sensor;

entering an identification number corresponding to the person seeking authorization into the POS terminal;

sending the identification number to the central computer in order to identify the stored fingerprint template corresponding to the identification number;

selecting the stored fingerprint template corresponding to the identification number and sending the stored template to the POS terminal; and

comparing the extracted minutiae information to the selected fingerprint template in the POS terminal.

37. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 36, further comprising the step of generating a signal based on results of the comparison between the extracted minutiae information and the stored fingerprint templates.

38. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 36, further comprising the step of encrypting the stored fingerprint template prior to sending it to the POS terminal.

39. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 36, further comprising the step of decrypting the stored fingerprint template sent by the central computer in the POS terminal.

40. A method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal comprising:

storing a fingerprint template of a person seeking authorization to initiate a transaction in an identification card prior to the initiation of the transaction;

transferring the stored fingerprint template from the card to the POS terminal using a card reader;

imaging a fingerprint of the person seeking authorization using a fingerprint sensor on the POS terminal;

extracting minutiae information from the image of the fingerprint captured by the fingerprint sensor on the POS terminal; and

comparing the extracted minutiae information to the stored fingerprint template using POS terminal circuitry.

41. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 40, wherein the image of the fingerprint generated by the fingerprint sensor in the smart card is in the form of a bitmap.

42. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 40, wherein the fingerprint template stored in the smart card is in the form of minutiae information corresponding to the person seeking authorization.

43. A method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal comprising:

storing a fingerprint template of a person seeking authorization to initiate a transaction in a smart card prior to the initiation of the transaction;

inserting the smart card into the POS terminal;

transferring the stored fingerprint template from the smart card to the POS terminal;

imaging a fingerprint of the person seeking authorization using a fingerprint sensor on the POS terminal;

extracting minutiae information from the image of the fingerprint captured by the fingerprint sensor on the POS terminal; and

comparing the extracted minutiae information to the stored fingerprint template using POS terminal circuitry.

44. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 43, wherein the image of the fingerprint generated by the fingerprint sensor in the POS terminal is in the form of a bitmap.

45. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 43, wherein the fingerprint template stored in the smart card is in the form of minutiae information corresponding to the person seeking authorization.

46. A method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal comprising:

storing a fingerprint template of a person seeking authorization to initiate a transaction in a smart card prior to the initiation of the transaction;

inserting the smart card into the POS terminal;

transferring the stored fingerprint template from the smart card to the POS terminal;

imaging a fingerprint of the person seeking authorization using a fingerprint sensor on the smart card;

extracting minutiae information from the image of the fingerprint captured by the fingerprint sensor on the smart card; and

comparing the extracted minutiae information to the stored fingerprint template using POS terminal circuitry.

47. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 46, wherein the image of the fingerprint generated by the fingerprint sensor in the smart card is in the form of a bitmap.

48. The method to authorize a transaction at a biometrically enabled point-of-sale (POS) terminal as in claim 46, wherein the fingerprint template stored in the smart card is in the form of minutiae information corresponding to the person seeking authorization.

FIG-1

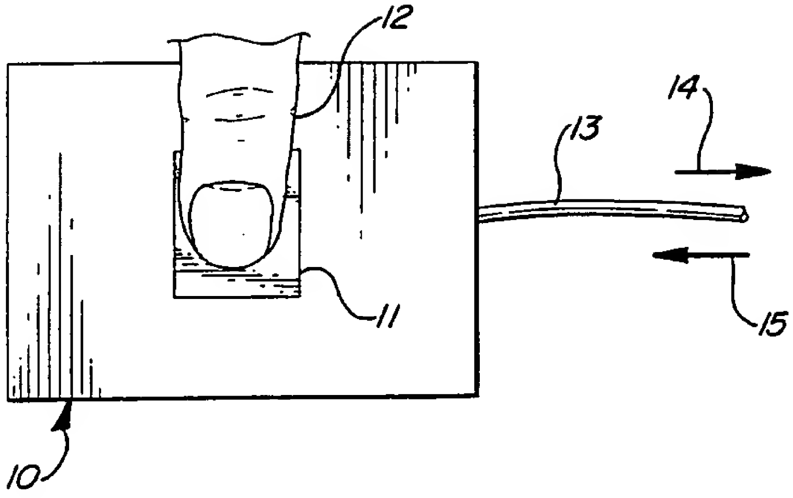


FIG-2

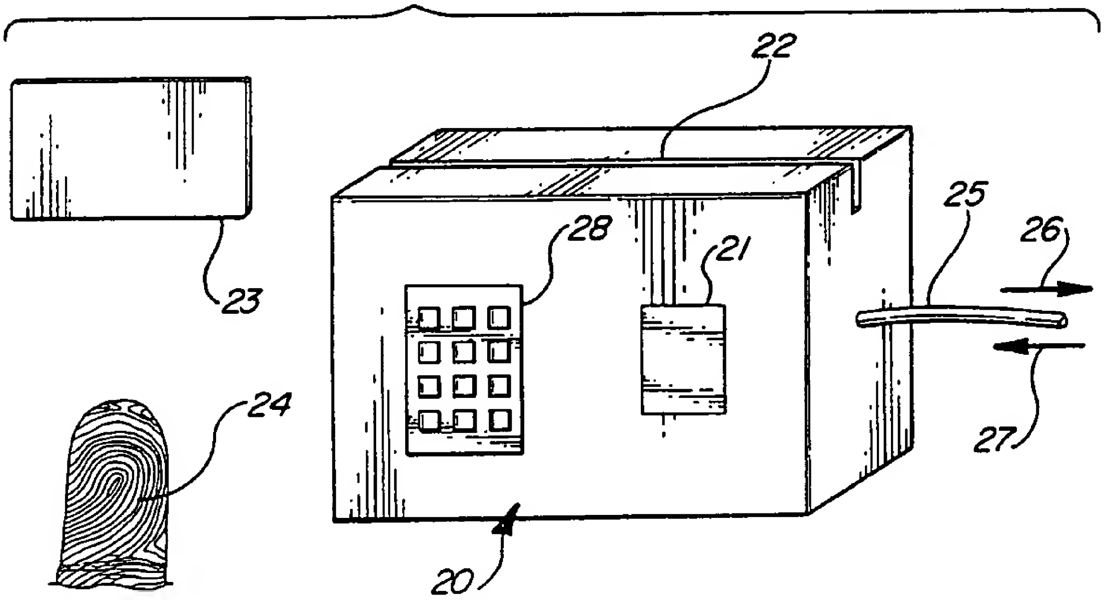


FIG-3

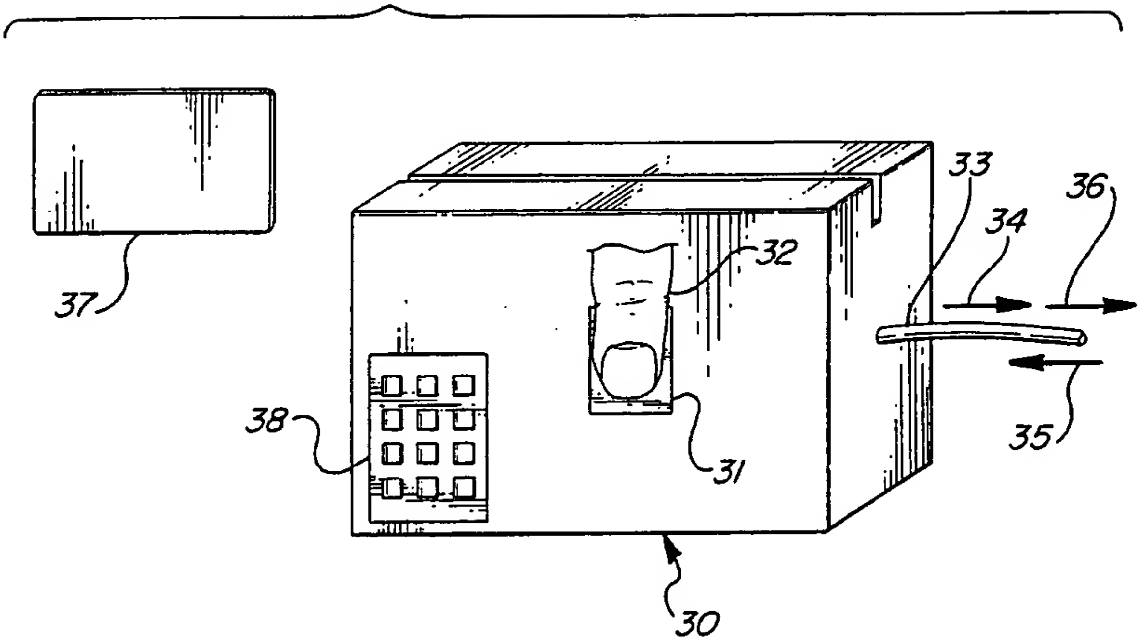
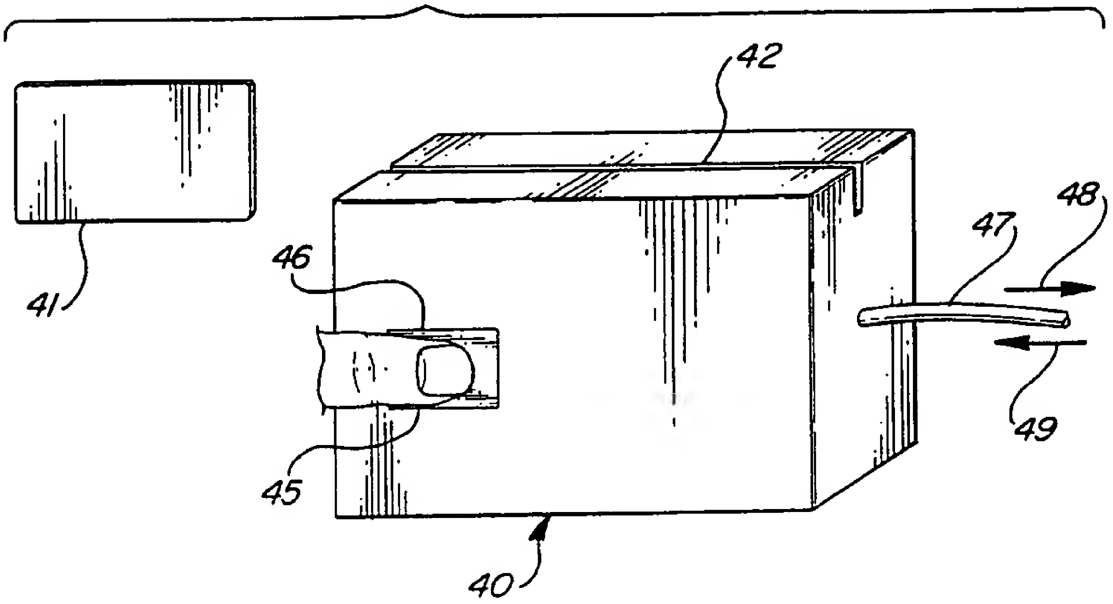


FIG-4A



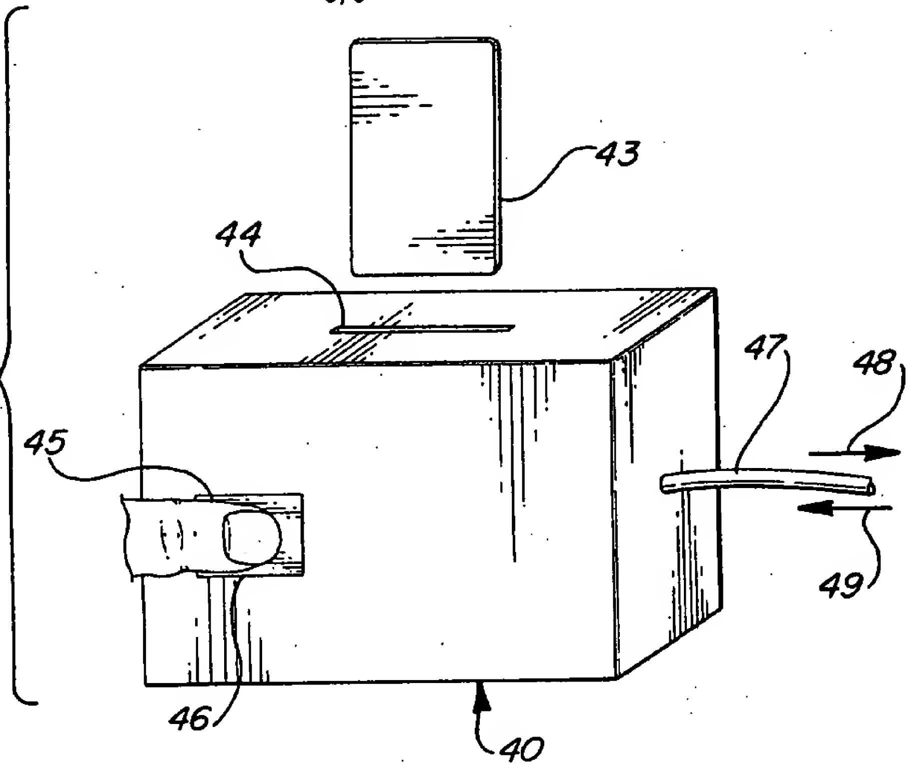


FIG-4B

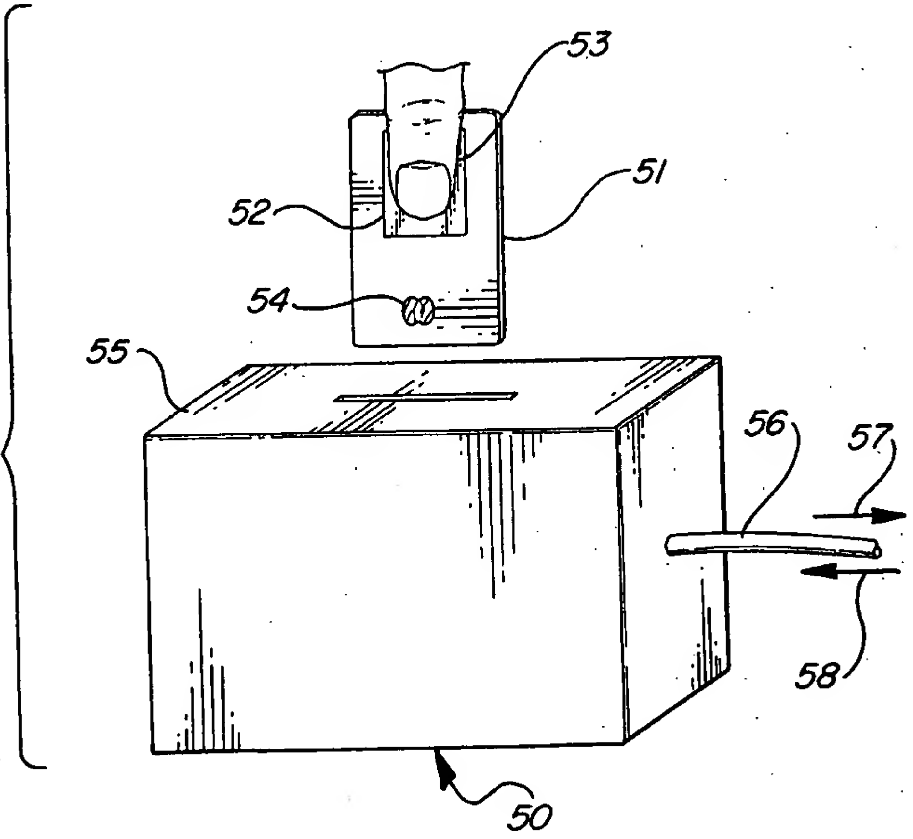


FIG-5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/07076

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06K 9/00
US CL :382/116, 125; 235/380
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 382/116, 125; 235/380

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST
search terms: smart card, fingerprint, minutiae, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,987,155 A (DUNN et al) 16 November 1999, abstract, Figure 2, col. 7, lines 3-55 and col. 8, lines 19-29.	1-48
Y	US 5,546,471 A (MERJANIAN) 13 August 1996, abstract, col. 9, line 13 - col. 10, line 58.	1-48
Y	US 5,615,277 A (HOFFMAN) 25 March 1997, abstract, Figure 1, col. 14, lines 14-30.	1-48

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search

02 JULY 2000

Date of mailing of the international search report

25 JUL 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
BHAVESH MEHTA
Eugenia Logan
Telephone No. (703) 308-3900